Fügen Sie Ihren eigenen Identitätsanbieter zu RevealX 360 hinzu

Veröffentlicht: 2024-07-02

Das RevealX 360-System enthält einen Standard-Identitätsanbieter (IdP), mit dem Sie Ihre Benutzer verwalten können , die auf das ExtraHop-System zugreifen. Wenn Ihr Unternehmen bereits über einen Identity Provider (IdP) verfügt, der Security Assertion Markup Language (SAML) 2.0 unterstützt, können Sie den IdP so konfigurieren, dass er Ihre Benutzer im ExtraHop-System verwaltet.

Um Ihren Identitätsanbieter hinzuzufügen, ordnen Sie Attribute für die Benutzeridentität und den Systemzugriff zwischen Ihrem IdP und dem ExtraHop-System zu und generieren eine Metadaten-XML-Datei, die das IdP-Zertifikat und die Attributinformationen enthält.

Hinweis: Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und Ihrem IdP kopieren und einfügen. Daher ist es hilfreich, jedes System nebeneinander zu öffnen.

Voraussetzungen

Bevor Sie Ihren Identitätsanbieter (IdP) hinzufügen, sollten Sie diese Überlegungen überprüfen.

System- und Identitätsanbieter

Überprüfen Sie diese System- und IdP-Anforderungen:

- Sie benötigen ein ExtraHop-Benutzerkonto mit System- und Zugriffsadministrationsrechten, um RevealX 360 zu konfigurieren.
- Identitätsanbieter müssen die folgenden Kriterien erfüllen:
  - SAML 2.0
  - Unterstützt SP-initiierte Anmeldeabläufe. IDP-initiierte Anmeldeabläufe werden nicht unterstützt.
  - Unterstützt signierte SAML-Antworten
  - Unterstützt HTTP-Redirect-Binding
- Sie müssen über ein gültiges Identitätsanbieter-Zertifikat verfügen. Wenn das Zertifikat abläuft, ist Single Sign-On an der ExtraHop RevealX 360-Konsole für alle Benutzer in Ihrer Organisation deaktiviert und Änderungen an der Systemkonfiguration schlagen fehl.

  Hinweis: Das ExtraHop-System sendet automatisch Benachrichtigungen über den Ablauf des IdP-Zertifikats an alle Benutzer mit System- und Zugriffsadministrationsrechte. E-Mails werden 1 Monat, 2 Wochen und 1 Woche vor dem Ablaufdatum des Zertifikats gesendet. Besorgen Sie sich ein neues Zertifikat von Ihrem Identitätsanbieter und aktualisiere deine IdP-Konfiguration.

SAML-Antworten

Stellen Sie sicher, dass alle SAML-Antworten die folgenden Bedingungen erfüllen:

- Antworten des SAML-Identitätsanbieters müssen eine Zielgruppenbeschränkung enthalten. Zum Beispiel:

```
<saml:AudienceRestriction>
  <saml:Audience>urn:amazon:cognito:sp:yourUserPoolID
</saml:AudienceRestriction>
```

- Die Antworten müssen einen enthalten `InResponseTo` Element in der `Response` Objekt, das der Anforderungs-ID in der Authentifizierungsanforderung entspricht. Zum Beispiel:

```
<samlp:Response ... InResponseTo="originalSAMLrequestId">
```

- EIN `SubjectConfirmationData` Attribut hat `Recipient` und `InResponseTo` eingestellte Werte. Zum Beispiel:

```
<saml:SubjectConfirmation>
  <saml:SubjectConfirmationData … Recipient="https://yourUserPoolDomain/
saml2/idpresponse" InResponseTo="originalSAMLrequestId">
</saml:SubjectConfirmation>
```

Weitere Informationen zur Konfiguration der Single Sign-On (SSO) -Authentifizierung für das ExtraHop-System über SAML-Identitätsanbieter finden Sie unter Konfigurieren Sie die Fernauthentifizierung über SAML.

Sehen Sie sich die Zugriffstypen und Rechtestufen von RevealX 360 an

Es gibt vier Zugriffstypen mit jeweils eigenen Berechtigungsstufen, die Sie Ihren Benutzern in RevealX 360 gewähren können: Benutzerberechtigungszugriff, Zugriff auf Pakete und Sitzungsschlüssel , Zugriff auf Network Detection and Response (NDR) -Module und Zugriff auf das Network Performance Management (NPM) -Modul.

Machen Sie sich mit den folgenden Zugriffstypen und den zugehörigen Berechtigungsstufen vertraut. In den Verfahren in diesem Handbuch ordnen Sie Attributnamen zwischen beiden Systemen zu.

siehe Benutzerrechte um zu erfahren, was Benutzer in den einzelnen Rechtestufen in RevealX 360 tun können.

Zugriff auf Benutzerrechte

Gewährt Benutzern Lese- und Schreibrechte im gesamten System. Es gibt 8 verfügbare Rechtestufen: System- und Zugriffsverwaltung, Systemadministration, Vollständiges Schreiben, Eingeschränktes Schreiben, Persönliches Schreiben, Vollständiges Lesen, Eingeschränktes Lesen und keine.

Zugriff auf Pakete und Sitzungsschlüssel

Ermöglicht Benutzern das Anzeigen und Herunterladen von Paketerfassungen mit oder ohne die Möglichkeit, Sitzungsschlüssel herunterzuladen: Kein Zugriff, nur Paketbereiche, Nur Pakete oder Pakete und Sitzungsschlüssel.

Zugriff auf das NDR-Modul

Gewährt Benutzern die Möglichkeit, Sicherheitserkennungen und Workflows einzusehen: Kein Zugriff oder Vollzugriff.

Zugriff auf das NPM-Modul

Gewährt Benutzern die Möglichkeit, Netzwerkleistungserkennungen und Workflows einzusehen: Kein Zugriff oder Vollzugriff.

Wenn Sie Ihren Benutzern nur Zugriff auf die Berechtigungsstufen Vollständig schreiben und Vollständig schreibgeschützt, kein Paketzugriff und vollständigen Erkennungszugriff gewähren möchten, erstellen Sie ein Arbeitsblatt, das dem folgenden Beispiel ähnelt:

Art des Zugriffs	Name der Berechtigungsstufe in RevealX 360	Attributwert in Ihrem IdP
Zugriff auf Benutzerrechte	Vollständig schreiben	Vollständiges Schreiben
Zugriff auf Benutzerrechte	Vollständig schreibgeschützt	Nur lesbar

Art des Zugriffs	Name der Berechtigungsstufe in RevealX 360	Attributwert in Ihrem IdP
Zugriff auf Pakete	Kein Zugriff	Keine
Zugriff auf das NDR-Modul	Voller Zugriff	Voller NDR
Zugriff auf das NPM-Modul	Voller Zugriff	Volles NPM

Fügen Sie Ihre IdP SAML-Anwendung zu RevealX 360 hinzu

1. Loggen Sie sich in RevealX 360 ein.
2. Klicken Sie auf Systemeinstellungen ⚙ oben rechts auf der Seite und klicken Sie dann auf **Die gesamte Verwaltung**.
3. Klicken Sie **Benutzerzugriff**.
4. Notieren Sie sich die URL und die Entitäts-ID des Assertion Consumer Service (ACS), die Sie in Ihre IdP-Konfiguration einfügen.
5. Fügen Sie die ACS-URL von RevealX 360 in das **ACS-URL** Feld auf deinem IdP.
6. Fügen Sie die SP Entity ID von RevealX 360 in das **SP-Entitäts-ID** Feld auf deinem IdP.

Nächste Schritte
Lassen Sie die IdP-Einstellungen geöffnet und konfigurieren Sie als Nächstes die Attributzuordnungen.

Konfigurieren Sie Attribute, die den Benutzer identifizieren

Sie müssen Attribute auf Ihrem IdP konfigurieren, die den Benutzer im gesamten ExtraHop-System anhand seines Vornamens, Nachnamens und seiner E-Mail-Adresse identifizieren. Die richtigen Eigenschaftsnamen beim Zuordnen dieser Attribute oder Attributangaben finden Sie in der Dokumentation Ihres Identitätsanbieters.

Führe die folgenden Schritte auf deinem IdP aus.

1. Fügen Sie im Abschnitt Zuordnung von Anwendungsattributen drei Attribute hinzu.
2. Wählen Sie im ersten Attribut **E-Mail senden** oder ähnlich. (In Okta heißt dieses Attribut beispielsweise **Benutzer.E-Mail**.)
3. Fügen Sie für den Service Provider die folgende Zeichenfolge ein: `urn:oid:0.9.2342.19200300.100.1.3`
4. Wählen Sie im zweiten Attribut **Nachname** oder ähnlich. (In Okta heißt dieses Attribut beispielsweise **Benutzer.Nachname**.)
5. Fügen Sie für den Service Provider die folgende Zeichenfolge ein: `urn:oid:2.5.4.4`
6. Wählen Sie im dritten Attribut **Vorname** oder ähnlich. (In Okta heißt dieses Attribut beispielsweise **Benutzer.Vorname**.)
7. Fügen Sie für den Service Provider die folgende Zeichenfolge ein: `urn:oid:2.5.4.42`

In Okta sollte der Abschnitt zur Attributzuordnung beispielsweise wie folgt aussehen:

Name des Dienstanbieter-Attributs (RevealX 360)	Name des Identitätsanbieter-Attributs (Okta)
`urn:oid:0.9.2342.19200300.100.1.3`	**Benutzer.E-Mail**
`urn:oid:2.5.4.4`	**Benutzer.Nachname**
`urn:oid:2.5.4.42`	**Benutzer.Vorname**

Konfiguration von Attributen für den Systemzugriff

Sie müssen Attribute auf Ihrem Identitätsanbieter konfigurieren, um Benutzern Zugriff auf das ExtraHop-System zu gewähren. Sie können einen beliebigen Namen für diese Attribute eingeben, sie müssen jedoch mit dem übereinstimmen, was Sie später in RevealX 360 konfigurieren.

Sie müssen mindestens ein Attribut für den Zugriff auf Benutzerrechte erstellen. Der Paket-, NDR- und NPM-Zugriff ist optional, wir empfehlen jedoch, diese Attribute jetzt zu erstellen.

Wichtig: Attributwerte müssen weniger als 2.000 Zeichen lang sein.

1. Fügen Sie im Abschnitt Zuordnung von Anwendungsattributen vier Attribute hinzu.
2. Wählen Sie im ersten Attribut Benutzerdefiniert oder ähnlich aus und geben Sie einen beschreibenden Namen für Benutzerrechte ein, z. B. `Level schreiben`.
3. Geben Sie für den Dienstanbieter einen beschreibenden Begriff ein, um das Attribut in RevealX 360 zu identifizieren, z. B. `schreiben`.
4. Wählen Sie im zweiten Attribut Benutzerdefiniert oder ähnlich aus und geben Sie einen beschreibenden Namen für den Paketzugriff ein, z. B. `Paketebene`.
5. Geben Sie für den Dienstanbieter einen beschreibenden Begriff ein, um das Attribut in RevealX 360 zu identifizieren, z. B. `Pakete`.
6. Wählen Sie im dritten Attribut Benutzerdefiniert oder ähnlich aus und geben Sie einen beschreibenden Namen für den NDR-Modulzugriff ein, z. B. `ndr-Niveau`.
7. Geben Sie für den Dienstanbieter einen beschreibenden Begriff ein, um das Attribut in RevealX 360 zu identifizieren, z. B. `ndr`.
8. Wählen Sie im vierten Attribut benutzerdefiniert oder ähnlich aus und geben Sie einen beschreibenden Namen für den NPM-Modulzugriff ein, z. B. `npm-Ebene`.
9. Geben Sie für den Dienstanbieter einen beschreibenden Begriff ein, um das Attribut in RevealX 360 zu identifizieren, z. B. `npm`.
10. Speichern Sie die Einstellungen und exportieren Sie dann die XML-Datei mit den Anwendungsmetadaten.

In Okta sollte der Abschnitt zur Attributzuordnung beispielsweise wie folgt aussehen:

Name des Dienstanbieter-Attributs (RevealX 360)	Name des Identitätsanbieter-Attributs (IdP)
`schreiben`	Level schreiben
`Pakete`	Paketebene
`ndr`	ndr-Niveau
`npm`	npm-Ebene

Konfigurieren Sie Ihre Identitätsanbieterinformationen in RevealX 360

Im Folgenden finden Sie einige Überlegungen, bevor Sie die folgenden Schritte ausführen. Stellen Sie sicher, dass Sie die Berechtigungsstufen identifiziert haben, die Sie Ihren Benutzern für jede Art von Systemzugriff gewähren möchten.

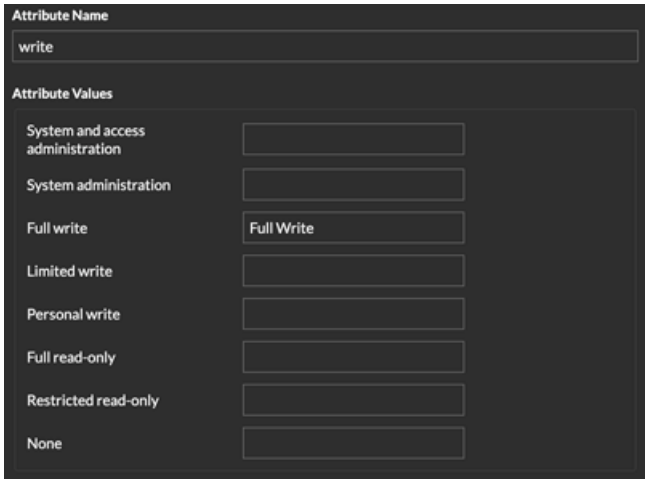
1. Klicken Sie in RevealX 360 auf der Seite Benutzerzugriff auf **Identitätsanbieter hinzufügen**.
2. In der **Name des Anbieters** Feld, geben Sie einen Namen ein, um Ihren spezifischen Identitätsanbieter zu identifizieren. Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems.

   Der Name muss den folgenden Richtlinien entsprechen:

   - Darf nur Punkte, Bindestriche und alphanumerische Zeichen enthalten
   - Muss zwischen 3 und 32 Zeichen lang sein

3. Öffnen Sie die Metadatendatei, die Sie im vorherigen Verfahren exportiert haben, und kopieren Sie dann den Inhalt und fügen Sie ihn in **Anbieter-Metadaten (XML)** Feld.
4. Scrollen Sie zum Attribute von Benutzerrechten Abschnitt. Es gibt drei Abschnitte, einen für jeden Zugriffstyp.
5. In der **Name des Attributs** Geben Sie in dieses Feld den Namen ein, den Sie auf Ihrem IdP für den Zugriff auf Benutzerrechte konfiguriert haben.
6. In unserem Beispiel oben haben wir spezifiziert `schreiben`. In der **Attributwerte** Felder, geben Sie die Namen der Berechtigungsstufen ein, die Sie für Ihre Benutzer identifiziert haben. In der folgenden Abbildung haben wir angegeben `Vollständiges Schreiben` für die **Volle Schreibrechte** Wert.

   Wichtig: Sie müssen angeben **Name des Attributs** und konfigurieren Sie mindestens einen anderen Attributwert als **Keine** um Benutzern die Anmeldung zu ermöglichen.



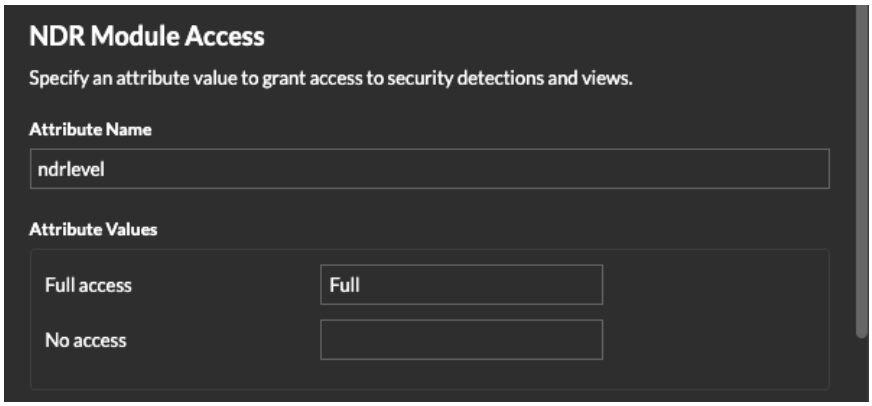
7. Scrollen Sie zum Zugriff auf Pakete und Sitzungsschlüssel Abschnitt.

   Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore haben. Wenn Sie keinen Packetstore haben, geben Sie ein `NA` in der **Name des Attributs** Feld und verlasse das **Attributwert** Felder leer.
8. In der **Name des Attributs** Geben Sie in dieses Feld den Namen ein, den Sie auf Ihrem IdP für den Paketzugriff konfiguriert haben. In unserem Beispiel oben haben wir angegeben `Pakete`.
9. In der **Attributwerte** Felder, geben Sie die Namen der Berechtigungsstufen ein, die Sie für Ihre Benutzer erstellt haben. In der folgenden Abbildung haben wir angegeben `Keine`.

10. Scrollen Sie zum Zugriff auf das NDR-Modul Abschnitt.

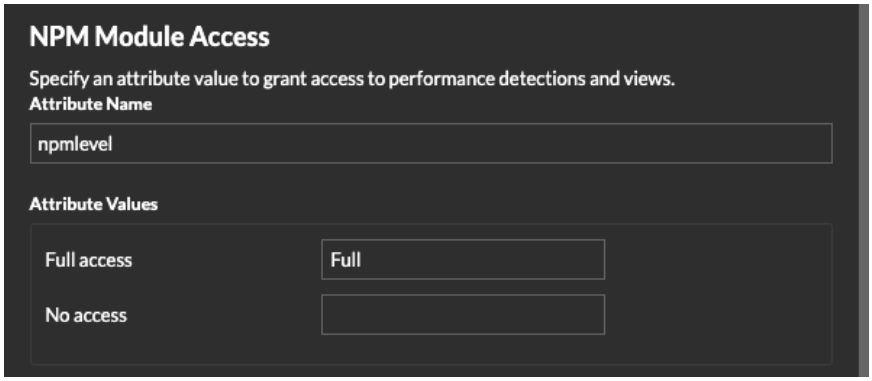
Konfigurieren Sie das NDR-Modulzugriffsattribut, wenn Sie möchten, dass Benutzer Zugriff auf Sicherheitserkennungen und Workflows haben. Andernfalls geben Sie NA in das **Name des Attributs** Feld und verlasse das **Attributwerte** Felder leer.

11. In der **Name des Attributs** Geben Sie in dieses Feld den Namen ein, den Sie auf Ihrem IdP für den Zugriff auf das NDR-Modul konfiguriert haben. In unserem Beispiel oben haben wir angegeben `ndr-Niveau`.
12. In der **Attributwerte** Felder, geben Sie die Namen der Berechtigungsstufen ein, die Sie für Ihre Benutzer erstellt haben. In der folgenden Abbildung haben wir angegeben `Voll`.



13. Scrollen Sie zum Zugriff auf das NPM-Modul Abschnitt.

    Konfigurieren Sie das NPM-Modulzugriffsattribut, wenn Sie möchten, dass Benutzer Zugriff auf Leistungserkennungen und Workflows haben. Andernfalls geben Sie NA in das **Name des Attributs** Feld und verlasse das **Attributwerte** Felder leer.
14. In der **Name des Attributs** Geben Sie in dieses Feld den Namen ein, den Sie auf Ihrem IdP für den NPM-Modulzugriff konfiguriert haben. In unserem Beispiel oben haben wir angegeben `npm-Ebene`.
15. In der **Attributwerte** Felder, geben Sie die Namen der Berechtigungsstufen ein, die Sie für Ihre Benutzer erstellt haben. In der folgenden Abbildung haben wir angegeben `Voll`.



16. klicken **Speichern**. Es kann bis zu zwei Minuten dauern, bis die IdP-Konfiguration gespeichert und auf dem System aktiviert ist.

Weisen Sie Benutzern in Ihrem IdP Rechte zu

Sie können Ihren bestehenden Benutzern jetzt Systemzugriffsattribute und die zugehörigen Berechtigungsstufen hinzufügen. Sie können einem Benutzer mehrere Rechte zuweisen, aber der Benutzer erhält immer die höchste Berechtigung, wenn er sich am System anmeldet.

Hinweis: Das ExtraHop-System unterstützt Gruppenattribut-Anweisungen, um Benutzerberechtigungen auf einfache Weise allen Mitgliedern einer bestimmten Gruppe zuzuordnen. Wenn Sie die ExtraHop-Anwendung auf Ihrem Identity Provider konfigurieren,

geben Sie einen Gruppenattributnamen an. Dieser Name wird dann in das Feld Attributname eingegeben, wenn Sie den Identity Provider auf dem ExtraHop-System konfigurieren.

1. Wählen Sie in Ihrem IdP den Benutzer aus, dem Sie Rechte gewähren möchten.
2. Fügen Sie ein Attribut für den zuvor definierten Zugriffstyp hinzu, z. B. writelevel.
3. Fügen Sie in derselben Zeile den Namen hinzu, den Sie für die Berechtigungsstufe angegeben haben, z. B. Full Write.

Die folgende Abbildung zeigt ein Beispiel für diese Attribute in JumpCloud:

Benutzer in RevealX 360 anzeigen

Benutzer werden auf der Benutzerseite in RevealX 360 angezeigt, nachdem sie sich das erste Mal angemeldet haben. Wenn ein Benutzer nicht in der Tabelle erscheint, wurde er nicht erfolgreich authentifiziert und autorisiert. Wenden Sie sich an den ExtraHop Support, wenn Sie Hilfe benötigen.

1. Loggen Sie sich in RevealX 360 ein.
2. Klicken Sie auf Systemeinstellungen oben rechts auf der Seite und klicken Sie dann auf **Die gesamte Verwaltung**.
3. Klicken Sie **Benutzerzugriff**. Benutzer, die sich erfolgreich am System anmelden, werden in der Tabelle auf der Benutzerseite in RevealX 360 angezeigt. In der Tabelle werden der Name des Identity Providers und die zugewiesenen Rechte für jeden Benutzer angezeigt.
4. Klicken Sie auf einen Benutzernamen, um Benutzerdetails anzuzeigen oder den Benutzer aus dem System zu löschen.

Wichtig: Wenn Sie einen Benutzer löschen, müssen Sie auch den Benutzerzugriff auf das ExtraHop-System über Ihren IdP widerrufen. Andernfalls kann sich der Benutzer möglicherweise erneut anmelden.

Einstellungen des Identitätsanbieters aktualisieren

Wenn Sie Änderungen an Ihrer Identitätsanbieter-Konfiguration vornehmen, z. B. das IdP-Zertifikat neu generieren, müssen Sie die neue Metadaten-XML-Datei exportieren und die Identitätsanbieter-Einstellungen auf RevealX 360 aktualisieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie unerwünschte Daten, wie z. B. ein abgelaufenes IdP-Zertifikat, aus der Metadaten-XML-Datei entfernen.

1. Loggen Sie sich bei Ihrem Identitätsanbieter ein.
2. Wählen Sie die ExtraHop-Anwendung auf Ihrem Identitätsanbieter aus und exportieren Sie die aktualisierte Metadaten-XML-Datei.
3. Öffnen Sie die XML-Datei in einem Texteditor und kopieren Sie den Inhalt.
4. Melden Sie sich bei RevealX 360 mit einem Benutzerkonto an, das über System- und Zugriffsadministrationsrechte verfügt.
5. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **Benutzerzugriff**.
6. In der SAML-Konfiguration Abschnitt, klicken Sie **Identity Provider bearbeiten**.
7. Fügen Sie den Inhalt der XML-Datei in das Anbieter-Metadaten XML Feld.
8. Klicken Sie **Speichern**.

Wichtig: Alle aktiven Benutzer werden nach dem Speichern der aktualisierten Konfiguration abgemeldet.